West Virginia Executive Branch
Privacy Tip of the Week

Know the Information Security Rules

Question:

Sometimes I'm not sure what information is really "protection worthy." Are there rules for keeping personally identifiable information safe?

Answer:

Everyone has access to lots of personally identifiable information (PII), such as geographical addresses, e-mail addresses and telephone numbers. In your job, you may have access to even more PII, like credit and debit card numbers or health information about private citizens and your co-workers. PII fills our buildings and our computer systems. Many interactions we have at work involve at least some PII. Because you have access to PII, you have an obligation to protect it. Understanding our information security rules is an important part of your job!

The Executive Branch Security Safeguards Policy requires each Department to protect the privacy, confidentiality, integrity and availability of PII.

- Privacy means that the PII won't be used for unintended or unauthorized purposes.
- Confidentiality means that the PII won't be disclosed to unauthorized individuals.
- Integrity means that the PII won't be changed or improperly deleted.
- Availability means that the PII will be accessible when it's needed.

Each Department must think about the ways that the privacy, confidentiality, integrity and availability of PII might be threatened, and then ensure that steps are taken to protect the PII from these threats. This includes PII in electronic format, as well as PII in paper records.

The West Virginia Office of Technology (WVOT) issues specific security rules. These rules are designed to protect our computer systems, as well as PII. You must understand all of the rules that apply to your activities. These rules are found at

WVOT's website at: http://www.technology.wv.gov/about-wvot/Pages/policies-issued-by-the-cto.aspx

The Security Safeguards Policy also describes the steps that must be taken when a security incident occurs. A security incident is any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any electronic information. If sensitive PII, i.e., Social Security numbers, financial account numbers, medical information, is exposed, the Security Safeguards Policy requires additional actions, such as consumer notification.

If you have questions about the Security Safeguards Policy or any privacy or security procedure, contact your Privacy or Security Officer.